Jim Carroll

Exposure a risk when security's neglected

If there is one thing that mystifies me about the world of IT, it has to be the absolute disrespect corporate organizations continue to pay to the issue of security.

Now, we all know that the issue of computer security can be a rather touchy subject, guaranteed to set off a range of emotions. Certainly I get frustrated with the way the mainstream media reports on technology-related security issues; frequent use of "shocking" headlines, inaccurate or dishonest reporting, and often, ridiculous hysteria. ("Credit cards aren't safe on the Internet!" "Code Red, Code Red!!!") Check my digitalsurvival.com site for an article in which I advise the media to "grow up" with respect to its reporting.

Now, don't get me wrong. We all know that there are big security problems in this technological world that surrounds us. Yes, the media went overboard with their reporting on potential problems from the Code Red situation. And yet, I'm writing this article more than a month after the Code Red scare, and I still see a large number of Web servers being infected on a regular basis, simply by examining my Web logs.

> While we continue to be inundated with new technologies, too many companies have too many clueless idiots who rush to put the latest and greatest stuff in place, all while ignoring the most basic security issues.

What is with these people? How can they possibly ignore what is going on? Why have they not downloaded the recommended security patches to reduce the risk on their Web servers? How can there be so many clueless people out there?

To me, it's a mystery. And it seems that sadly, while we continue to be inundated with new technologies, too many companies have too many clueless idiots who rush to put the latest and greatest stuff in place, all while ignoring the most basic security issues.

Take the world of wireless. One of the most exciting technologies that have come out in the last few years is the 802.11b networking standard, also known as Wi-Fi. It allows companies to avoid costly wired LANs — instead, you get a full 11Mbs right out of the air by using a wireless LAN card, which links into a wireless LAN hub.

It works, and it is fabulous. I've got a 3Com 802.11b 3Com wireless LAN in my home, which allows me to use my laptop from literally anywhere in the house, and indeed, throughout my neighbourhood. (I'm sort of the neighbourhood Mr. Fix-it when it comes to computers — I'm regularly running here and there to solve problems that my technically challenged neighbours have with their PCs.) The technology allows me to take my laptop with me, and pull necessary drivers and software patches "out of the air," so to speak. I'm good for a few hundred feet at least!

Because it is such an exciting technology, usage of Wi-Fi is literally exploding out of the gate within the corporate sector. And yet while they are rushing to put this technology in place, many are ignoring the issue of security, most often by not undertaking the most common security steps of changing default passwords, putting in place recommended encryption, locking down access to specific known hardware devices, and other recommended steps.

How bad is it? Over at Extreme Computing.com, there's a fabulous article that puts into perspective the security exposures that exist. (Do a search for the article "Exploiting and protecting 802.11b Wireless Networks. Yes, wireless LANs are vulnerable, but yours doesn't have to be.") Basically, the article outlines how two fellows drove through Manhattan with a Linux-laptop, some sniffer software and a couple of sophisticated antennas. Their goal was to see how many wireless corporate networks they could discover that had security exposures.

The results are kind of stunning — it took them but a matter of minutes to find more than 60 wide-open corporate LANs. We're not talking LANs that they might be able to crack with some sophisticated decryption software — but LANs that they could easily logon to, or which were still using default administrative passwords. LANs, which were for all intents and purposes, just waiting to be accessed by anyone with a laptop and a wireless LAN card.

> Haven't we known for thirty years that this is something you MUST DO every time you implement a new system? Will people never learn? Sadly, the answer seems to be "no."

Why is the problem so bad? Primarily, because the people who have installed this technology hadn't even bothered changing the default user ID and password required for administrative access. Yet hasn't that long been one of the basic, recommended, most fundamental security procedures? Haven't we known for thirty years that this is something you MUST DO every time you implement a new system?

Will people never learn? Sadly, the answer seems to be "no."

Anyone involved with technology must become conversant with security issues. In my case, as soon as I installed my own Wi-Fi hardware a year or so ago, I took the time to learn about the security issues that surround Wi-Fi and my own particular hardware, and did what I could to clamp down on those risks. I feel relatively comfortable at this point that if someone was trying to break into my system, they wouldn't have much luck. (And no, I don't issue that as a challenge!) Yet sadly, my inherent technological curiosity means that I was willing to undertake such a time investment. Many others do not.

Wi-Fi is but one new technology — and given the massive inroads that this technology is making into the corporate world, it is likely that there will continue to be a constant stream of break-ins, security violations, and other problems. The media is going to have a field day with this. The result is that we will see ongoing media hysteria, significant corporate problems, and a resultant continued public mistrust in our global technology infrastructure.

And this is but one example. I don't even want to think about the potential security flaws that might be creeping into the e-commerce sites that involve significant middleware coding. All over the world, companies are busy linking their Web sites to their back-end information systems, and are using a smorgasbord of methods to do so. Imagine the coding problems, security holes and other problems that are already in existence out there, simply because many of these initiatives will ignore security until it is far too late.

So while I bemoan the media hysteria that creeps into the topic of security, I continue to be amazed that companies and people continue to ignore the issue. Sadly, I expect things to get worse before they get better. «

Jim Carroll is an author, columnist and frequent keynote speaker who focuses on the impact and challenges of the digital age. His Web site can be found at www.jimcarroll.com.